UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,931	12/15/2003	Steven Tischer	030515 (BLL-0144)	3718

36192 7590 04/16/2008

CANTOR COLBURN LLP - BELLSOUTH
20 Church Street
22nd Floor
Hartford, CT 06103

EXAMINER	
HAILE, AWET A	

ART UNIT	PAPER NUMBER
2616	

MAIL DATE	DELIVERY MODE
04/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/735,931	TISCHER, STEVEN	
	Examiner	Art Unit	
	AWET HAILE	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-15 and 17-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-15 and 17-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. **Claims 1-4, 6-15 and 17-21** are pending on this application.

2. **Claims 5 and 16** are cancelled.

Response to Argument

3. Applicant's arguments with respect to claims **1-4, 6-15 and 17-21** have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections – 35 USC§ 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. **Claims 1-4, 6,7,11-15, 17, 18 and 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over Labaton et al (US 5742684) in view of Candelore (US 2002/0095580 A1).

Regarding claim 1, Labaton'684 discloses, a method for transmitting data over a computer network to a predetermined recipient (Fig 1, transmitting bank card information from special tone dialer(STD) unit 16 to the host computer 28), the method comprising: modifying at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message(column 5, lines 10-13, notice, the card information is encrypted using the current time(GMT) as an encryption key), the first message modification key value being determined based on at least one variable parameter(column 5, lines 10-13, Greenwich Mean Time(GMT));

modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (column 6, lines 59-67, encrypting the next message using the changing GMT as an encryption key), the second message modification key value being determined based on at least one variable parameter (column 6, lines 59-67, notice the time changes every second, and this changing time is used for encryption);

transmitting the first and second modified data messages to a first device(Fig 1, transmitting encrypted bank card information from special tone dialer unit 16 to the host computer 28);determining the first data message in the first device for the predetermined recipient based on the modified first data message and the first message modification key value(

column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving interface computer 26 in order to use it as a decryption key); and determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value(column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26, which is different from the previously sent GMT);

wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message (column 6, line 60 - column 7 line 5, notice, the encryption algorithm updates every minute (GMT), thus, STD 16 encrypt data packets that are going to be transmitted within a minute using the same encryption key (GMT));

Wherein the first message modification key value being determined based on the at least one variable parameter (GMT) and a unique identifier associated with the predetermined recipient (column 5, lines 14-19, since the PIN number is used to access the user account information stored in the host computer 28, the PIN number is associated with the recipient host computer 28).

However, Labaton'684, failed to teach, the unique identifier being a biometric identifier obtained from the recipient.

Candelore'580 teaches, the unique identifier being a biometric identifier obtained from the recipient(paragraph 28, notice, a biometric data is used as an encryption key along with other variables, see also Fig, 2 step 203).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using a biometric data as an encryption key as taught by Candelore'580 into the encryption method of Labaton'684, in order to prevent fraudulent use of a device, since such method is suggested by Candelore'580(paragraph 25).

Regarding claim 2, Labaton'684 discloses, wherein the variable parameter comprises a time- varying parameter (column 6, line 60-67, changing the encryption algorithm periodically).

Regarding claim 3, Labaton'684 discloses, wherein the time-varying parameter includes at least one of a determined hour, minute, and second (see column 5, lines 10-12, GMT is used as an encryption key).

Regarding claim 4, Labaton'684 failed to teach, recipient biometric identifier obtained from the recipient is a voice sample of the recipient.

However, Candelore'580 teaches, recipient biometric identifier obtained from the recipient is a voice sample of the recipient (paragraph 28, lines 6-9, a voice sample is used for encryption).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using a biometric (voice sample) data as an encryption key as taught by Candelore'580 into the encryption method of Labaton'684, in order to prevent fraudulent use of a device, since such method is suggested by Candelore'580 (paragraph 25).

Regarding claim 6, Labaton'684 discloses, transmitting the first and second message modification key values to a first computer(column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26 in order to use it as a decryption key).

Regarding claim 7, Labaton'684 discloses, wherein the first and second modified data messages are both transmitted via a first communication channel (fig 1, transmission line 24, the encrypted data is transmitted via transmission line 24).

Regarding claim 11, Labaton'684 discloses, a system for transmitting data over a computer network to a predetermined recipient (Fig 1, transmitting bank card information from special tone dialer unit 16 to the host computer 28), the system comprising:

a first device configured to modify at least one data byte in a first data message based on a first message modification key value to obtain a modified first data message (column 5, lines 10-13, notice, the card information is encrypted using the current time (GMT) as an encryption

key), the first message modification key value being determined based on at least one variable parameter (column 5, lines 10-13, Greenwich Mean Time (GMT));

the first device further configured to modify at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (column 6, lines 59-67, encrypting the next message using different GMT as an encryption key), the second message modification key value being determined based on at least one variable parameter (column 6, lines 59-67, notice the time changes every second, and this changing time is used for encryption);

the first device configured to transmit the first and second modified data messages(Fig 1, transmitting encrypted bank card information from special tone dialer unit 16 to the host computer 28); and a second device configured to receive the transmitted first and second modified data messages and to determine the first data message for the predetermined recipient based on the modified first data message and the first message modification key value(column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26 in order to use it as a decryption key);

the second device further configured to determine the second data message for the predetermined recipient based on the modified second data message and the second message modification key value(column 6 lines 34-40, notice: the time at which the card information

encrypted is transmitted to the receiving host computer 26, which is different from the previously sent GMT);

wherein the first device is configured to modify multiple bytes of a first data message by adding the first message modification key byte value to multiple bytes of the first data message (column 6, line 60 - column 7 line 5, notice, the encryption algorithm updates every minute (GMT), thus, STD 16 encrypt data packets that are going to be transmitted within a minute with the same encryption key (GMT));

wherein the first message modification key value is determined based on the at least one variable parameter and a unique identifier associated with the predetermined recipient(column 5, lines 14-19, since the PIN number is used to access the user account information stored in the host computer 28, the PIN number is associated with the recipient host computer 28).

However, Labaton'684, failed to teach, the unique identifier being a biometric identifier obtained from the recipient.

Candelore'580 teaches, the unique identifier being a biometric identifier obtained from the recipient(paragraph 28, notice, a biometric data is used as an encryption key along with other variables, see also Fig, 2 step 203).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using a biometric data as an encryption key as taught by Candelore'580 into the encryption method of Labaton'684, in order to prevent fraudulent use of a device, since such method is suggested by Candelore'580(paragraph 25).

Regarding claim 12, Labaton'684 discloses, wherein the first and second devices comprise first (Fig 1, STD 16) and second computers (Fig 1, interface computer 26), respectively, operatively communicating with one another (Fig 1, STD 16 and interface computer 26 connected to each other).

Regarding claim 13, Labaton'684 discloses, wherein the variable parameter comprises a time- varying parameter (column 6, line 60-67, changing the encryption algorithm periodically).

Regarding claim 14, Labaton'684 discloses, wherein the time-varying parameter includes at least one of a determined hour, minute, and second (see column 5, lines 10-12, GMT is used as an encryption key).

Regarding claim 15, Labaton'684 failed to teach, recipient biometric identifier obtained from the recipient is a voice sample of the recipient.

However, Candelore'580 teaches, recipient biometric identifier obtained from the recipient is a voice sample of the recipient (paragraph 28, lines 6-9, a voice sample is used for encryption).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using a biometric (voice sample) data as an encryption key as taught by Candelore'580 into the encryption method of Labaton'684, in order to prevent fraudulent use of a device, since such method is suggested by Candelore'580 (paragraph 25).

Regarding claim 17, Labaton'684 discloses, wherein the first device is further configured to transmit the first and second message modification key values to the second device (column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26 in order to use it as a decryption key).

Regarding claim 18, Labaton'684 discloses, wherein the first and second modified data messages are both transmitted via a first communication channel (fig 1, transmission line 24, the encrypted data is transmitted via transmission line 24).

Regarding claim 21, Labaton'684 discloses, a method for transmitting data over a computer network to a predetermined recipient (Fig 1, transmitting bank card information from special tone dialer unit 16 to the host computer 28), the method comprising: modifying at least

one data byte in a first data message based on a first message modification key value to obtain a modified first data message(column 5, lines 10-13, notice, the card information is encrypted using the current time(GMT) as an encryption key), the first message modification key value being determined based on at least one variable parameter(column 5, lines 10-13, Greenwich Mean Time(GMT));

modifying at least one data byte in a second data message based on a second modification key value to obtain a modified second data message (column 6, lines 59-67, encrypting the next message using changing GMT as an encryption key), the second message modification key value being determined based on at least one variable parameter (column 6, lines 59-67, notice the time changes every second, and this changing time is used for encryption);

transmitting the first and second modified data messages to a first device(Fig 1, transmitting encrypted bank card information from special tone dialer unit 16 to the host computer 28);determining the first data message in the first device for the predetermined recipient based on the modified first data message and the first message modification key value(column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26 in order to use it as a decryption key); and determining the second data message in the first device for the predetermined recipient based on the modified second data message and the second message modification key value(column 6 lines 34-40, notice: the time at which the card information encrypted is transmitted to the receiving host computer 26, which is different from the previously sent GMT);

wherein the modifying at least one byte of the first data message includes adding the first message modification key byte value to multiple data bytes of the first data message (column 6, line 60 - column 7 line 5, notice, the encryption algorithm updates every minute (GMT), thus, STD 16 encrypt data packets that are going to be transmitted within a minute with the same encryption key (GMT));

Wherein the first message modification key value being determined based on the at least one variable parameter (GMT) and a unique identifier associated with the predetermined recipient (column 5, lines 14-19, since the PIN number is used to access the user account information stored in the host computer 28, the PIN number is associated with the recipient host computer 28).

However, Labaton'684, failed to teach, the unique identifier being a biometric identifier obtained from the recipient.

Candelore'580 teaches, the unique identifier being a biometric identifier obtained from the recipient(paragraph 28, notice, a biometric data is used as an encryption key along with other variables, see also Fig, 2 step 203).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of using a biometric data as an encryption key as

taught by Candelore'580 into the encryption method of Labaton'684, in order to prevent fraudulent use of a device, since such method is suggested by Candelore'580(paragraph 25).

7. **Claim 8-10, 19 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Labaton'684 and Candelore'580 as applied to **claims 1 and 11** above, and further in view of Kamperman et al(US 2002/0004903 A1).

Regarding claim 8, Labaton'684 and Candelore'580 failed to teach, wherein the first and second message modification key values are both transmitted via a second communication channel.

However, Kamperman'903 teaches, wherein the first and second message modification key values are both transmitted via a second communication channel (see paragraph 9, notice, kamperman'903 teaches, method of transmitting the encryption key and the encrypted data separately).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encryption key and encrypted data on a separate channel as taught by Kamperman'903 in to the STD 16 of Labaton'684, in order to send the encryption key quicker, so that in the receiving device all key codes for decryption and accessing the content is already available, since such a method is suggested by Kamperman'903(paragraph 9).

Regarding claim 9, Labaton'684 and Candelore'580 failed to teach, wherein said first data message comprises voice data.

However, Kamperman'903 teaches, wherein said first data message comprises voice data (see paragraph 29, Kamperman teaches a method of transmitting encrypted audio/ video signal to a user via a network).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encrypted audio/video data over a network as taught by Kamperman'903 into the communication system of Labaton'684, for controlled distribution of digital information, since such a method is suggested by Kampeman'903(paragraph 9).

Regarding claim 10, Labaton'684 and Candelore'580 failed to teach, wherein said first data message comprises video data.

However, Kamperman'903 teaches, wherein said first data message comprises video data (see paragraph 29, Kamperman teaches a method of transmitting encrypted audio/ video signal to a user via a network).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encrypted audio/video data over a

network as taught by Kamperman'903 into the communication system of Labaton'684, for controlled distribution of digital information, since such a method is suggested by Kampeman'903(paragraph 9).

Regarding claim 19, Labaton'684 and Candelore'580 failed to teach, wherein said first data message comprises voice data.

However, Kamperman'903 teaches, wherein said first data message comprises voice data (see paragraph 29, Kamperman teaches a method of transmitting encrypted audio/ video signal to a user via a network).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encrypted audio/video data over a network as taught by Kamperman'903 into the communication system of Labaton'684, for controlled distribution of digital information, since such a method is suggested by Kampeman'903(paragraph 9).

Regarding claim 20, Labaton'684 and Candelore'580 failed to teach, wherein said first data message comprises video data.

However, Kamperman'903 teaches, wherein said first data message comprises video data (see paragraph 29, Kamperman teaches a method of transmitting encrypted audio/ video signal to a user via a network).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate, the method of transmitting encrypted audio/video data over a network as taught by Kamperman'903 into the communication system of Labaton'684, for controlled distribution of digital information, since such a method is suggested by Kampeman'903(paragraph 9).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Ehrsam et al (3958081), Wheeler et al (20002/0116608 A1), Subramaniam et al (2004/0039702 A1), Mauritz et al (6853620 B2), Hamlin (7215771 B1), Pyle et al (US 2007/0005955 A1), Anderson(US 2005/0257055 A1) and Bianchi(US 2004/0059921 A1)are recited to show a method of transmitting data over a computer network.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to AWET HAILE whose telephone number is (571)270-3114. The examiner can normally be reached on Monday through Friday 8:30 AM - 4:30 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOE AUNG can be reached on (571)272-3474. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AWET HAILE
Examiner
Art Unit 2616

/Aung S. Moe/
Supervisory Patent Examiner, Art Unit 2616